

Introduced by Senator Bowen

February 24, 2006

An act to amend Section 1798.29 and 1798.82 of the Civil Code, relating to information privacy.

LEGISLATIVE COUNSEL'S DIGEST

SB 1744, as introduced, Bowen. Information privacy.

Existing law requires any agency, or a person or business conducting business in California, which owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

The bill would require that an agency or a person or business that has suffered a breach of the security of the system to provide 1 year of a credit monitoring service, as defined, without charge to each person whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Vote: majority. Appropriation: no. Fiscal committee: yes.
State-mandated local program: no.

The people of the State of California do enact as follows:

- 1 SECTION 1. Section 1798.29 of the Civil Code, as added by
- 2 Section 2 of Chapter 1054 of the Statutes of 2002, is amended to
- 3 read:
- 4 1798.29. (a) Any agency that owns or licenses computerized
- 5 data that includes personal information shall disclose any breach
- 6 of the security of the system following discovery or notification

1 of the breach in the security of the data to any resident of
2 California whose unencrypted personal information was, or is
3 reasonably believed to have been, acquired by an unauthorized
4 person. The disclosure shall be made in the most expedient time
5 possible and without unreasonable delay, consistent with the
6 legitimate needs of law enforcement, as provided in subdivision
7 (c), or any measures necessary to determine the scope of the
8 breach and restore the reasonable integrity of the data system.

9 (b) Any agency that maintains computerized data that includes
10 personal information that the agency does not own shall notify
11 the owner or licensee of the information of any breach of the
12 security of the data immediately following discovery, if the
13 personal information was, or is reasonably believed to have been,
14 acquired by an unauthorized person.

15 (c) The notification required by this section may be delayed if
16 a law enforcement agency determines that the notification will
17 impede a criminal investigation. The notification required by this
18 section shall be made after the law enforcement agency
19 determines that it will not compromise the investigation.

20 (d) For purposes of this section, “breach of the security of the
21 system” means unauthorized acquisition of computerized data
22 that compromises the security, confidentiality, or integrity of
23 personal information maintained by the agency. Good faith
24 acquisition of personal information by an employee or agent of
25 the agency for the purposes of the agency is not a breach of the
26 security of the system, provided that the personal information is
27 not used or subject to further unauthorized disclosure.

28 (e) For purposes of this section, “personal information” means
29 an individual’s first name or first initial and last name in
30 combination with any one or more of the following data
31 elements, when either the name or the data elements are not
32 encrypted:

33 (1) Social security number.

34 (2) Driver’s license number or California Identification Card
35 number.

36 (3) Account number, credit or debit card number, in
37 combination with any required security code, access code, or
38 password that would permit access to an individual’s financial
39 account.

(f) For purposes of this section, “personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section, “notice” may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the agency has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the agency’s Web site page, if the agency maintains one.

(C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(i) An agency that has suffered a breach of the security of the system shall provide one year of a credit monitoring service without charge to each person whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. For the purposes of this section, “credit monitoring service” means a service that allows a consumer electronic access to the information in his or her credit report on demand and provides regular E-mail notifications of changes to the consumer’s credit report.

SEC. 2. Section 1798.82 of the Civil Code, as added by Section 4 of Chapter 1054 of the Statutes of 2002, is amended to read:

1798.82. (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, “breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, “personal information” means an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

1 (2) Driver's license number or California Identification Card
2 number.

3 (3) Account number, credit or debit card number, in
4 combination with any required security code, access code, or
5 password that would permit access to an individual's financial
6 account.

7 (f) For purposes of this section, "personal information" does
8 not include publicly available information that is lawfully made
9 available to the general public from federal, state, or local
10 government records.

11 (g) For purposes of this section, "notice" may be provided by
12 one of the following methods:

13 (1) Written notice.

14 (2) Electronic notice, if the notice provided is consistent with
15 the provisions regarding electronic records and signatures set
16 forth in Section 7001 of Title 15 of the United States Code.

17 (3) Substitute notice, if the person or business demonstrates
18 that the cost of providing notice would exceed two hundred fifty
19 thousand dollars (\$250,000), or that the affected class of subject
20 persons to be notified exceeds 500,000, or the person or business
21 does not have sufficient contact information. Substitute notice
22 shall consist of all of the following:

23 (A) E-mail notice when the person or business has an e-mail
24 address for the subject persons.

25 (B) Conspicuous posting of the notice on the Web site page of
26 the person or business, if the person or business maintains one.

27 (C) Notification to major statewide media.

28 (h) Notwithstanding subdivision (g), a person or business that
29 maintains its own notification procedures as part of an
30 information security policy for the treatment of personal
31 information and is otherwise consistent with the timing
32 requirements of this part, shall be deemed to be in compliance
33 with the notification requirements of this section if the person or
34 business notifies subject persons in accordance with its policies
35 in the event of a breach of security of the system.

36 (i) *A person or business that has suffered a breach of the*
37 *security of the system shall provide one year of a credit*
38 *monitoring service without charge to each person whose*
39 *personal information was, or is reasonably believed to have*
40 *been, acquired by an unauthorized person. For the purposes of*

1 *this section, “credit monitoring service” means a service that*
2 *allows a consumer electronic access to the information in his or*
3 *her credit report on demand and provides regular E-mail*
4 *notifications of changes to the consumer’s credit report.*

O